CLAIMS:

1. A public key encryption scheme using a private key, z, and a public key, h, comprises the encryption of a message, m, within a ciphertext, wherein an element of the encrypted ciphertext containing the message is formed by a message product of a variable, ϵ, based on the public key, h, and an output of an invertible deterministic method, π, operated on at least the message, m, and a hash, H, of at least the message.

2. A public key encryption scheme as claimed in claim 1, wherein the ciphertext includes at least one random element, u_1.

3. A public key encryption scheme as claimed in claim 1, wherein the invertible deterministic method is operated on the message, m, an index, j, of the hash and a hash, H, over both the message, m, and at least one random element, u_1.

4. A public key encryption scheme as claimed in claim 1, wherein the variable, ϵ, based on the public key is the public key, h, raised to the power of a random number, r.

5. A public key encryption scheme as claimed in claim 1, wherein the ciphertext is decrypted using a private key, z, the at least one random element u_1, the message product, and the invertible deterministic method, π.

6. A public key encryption scheme as claimed in claim 1, wherein the invertible deterministic method, π, is operated on a check for the decryption.

7. A public key encryption scheme as claimed in claim 6, wherein, the hash, H, for the check is over the message and at least one random element, u_1.

8. A public key encryption scheme as claimed in claim 1, wherein the message product is represented by $\epsilon.M$, where $\epsilon = h^r$ (r is random) and $h = g_1^z$, where g_1 is a first generator, z is a randomly chosen private key and $M = \pi(m, j, t)$ where π is the

invertible deterministic method, m is the message, j is a random index of the hash and $t = H_j(m, g_1^r, g_2^r)$, where H_j is the j^{th} hash and g_2 is a second generator.

9. A public key encryption scheme as claimed in claim 1, wherein the ciphertext includes said at least one random element, u_1.

10. A public key encryption scheme as claimed in claim 1, wherein at least one of said random elements, u_1, is used to decipher the ciphertext, in conjunction with the private key, z, to determine the output, M, of the invertible deterministic method, π, which output is then inverted to give an original input and hence the message, m.

11. A public key encryption/decryption method makes use of a ciphertext that includes a check element, t, wherein a check made during decryption is a hash, H, over at least the encrypted message, m.

12. A public key encryption/decryption method as claimed in claim 11, wherein the hash, H, is over the message, m, and at least one random element, u_1.

13. A public key encryption method includes creating a ciphertext requiring at most 4 exponentiations to encrypt, including exponentiations for each of at least two random elements, u_1, u_2 and an exponentiation for a public key, h, wherein a message for encryption does not require an exponentiation to encrypt.

14. A public key encryption method as claimed in claim 13, wherein the method includes 3 exponentiations, being for a first random element, u_1, a second random element, u_2, and for the public key, h.

15. A public key encryption/decryption method includes decrypting a ciphertext with at most 2 exponentiations, including an exponentiation using a private key, z, to allow recovery of an encrypted message, m.

16. A public key encryption/decryption method as claimed in claim 15, wherein only one exponentiation is required.

17. A public key encryption/decryption method involves creating a ciphertext and decrypting the ciphertext, in which a public key requires no more than 3 group elements and a private key requires no more than one group element, whilst still providing a provably secure method.